

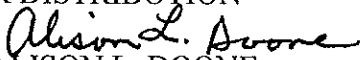


**Department of Energy**  
Washington, DC 20585

April 5, 2013

MEMORANDUM FOR DISTRIBUTION

FROM:

  
ALISON L. DOONE  
DEPUTY CHIEF FINANCIAL OFFICER

SUBJECT:

Fiscal Year (FY) 2013 Internal Control Evaluations Guidance

This memorandum and attachments provide guidance on the process to be implemented by Departmental elements and management and operating contractors to meet the evaluation requirements of the Federal Managers' Financial Integrity Act (FMFIA), as described in the Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Internal Control*. FMFIA and OMB Circular A-123 require annual self-assessment and reporting to the President and Congress on the status of internal controls.

The attached guidance provides instructions for conducting FY 2013 internal control evaluations in compliance with FMFIA and OMB Circular A-123 and will help ensure that the Secretary's annual Statement of Assurance is accurate and adequately supported. The results of Departmental element's FMFIA evaluations will be reported in an annual Assurance Memorandum, which will be due from field elements on August 2, 2013, and from Headquarters elements on September 3, 2013.

In FY 2012, the Department had a qualified opinion on the annual Statement of Assurance on internal controls because of the breach in security at the Y-12 National Security Complex. The breach revealed a systemic problem in processes at the site and a significant breakdown in non-financial internal controls. Consequently, the attached guidance emphasizes the importance of non-financial risks and internal controls while performing the assessment activities. We have expanded the risk assessment section of the guidance (Section V) to include additional information on assessing the risk of non-financial controls.

The attached guidance reiterates senior management's responsibility for quality assurance over the internal control program, including contractor internal controls. Management is responsible for ensuring the Federal organizations and contractor sites under their oversight comply with the attached guidance, including conducting adequate risk assessments, executing testing plans with appropriate sample sizes, and documenting final results.

We have modified the guidance addressing systems to address the evaluation criteria for core financial systems (Section IX) and mixed information systems (Section X). The modification removed the requirement of testing mixed information systems for criteria that are only applicable to core financial systems.



Finally, the guidance has a new section on evaluating the results of control assessments (Section VI). Regardless of the acceptable threshold established by management and the number of exceptions noted in testing internal controls, management needs to assess the exposure that *any* exception creates for the organization to determine the results. For example, with high-risk processes, one exception could have a significant impact on the organization, and therefore, needs to be assessed to determine if one failure should be reported as a material weakness.

We appreciate your cooperation and assistance as we fulfill the Department's internal control assurance responsibilities. If you have questions or want to discuss the requirements set forth in this memorandum or the guidance, please contact April G. Stephenson, Director, Office of Financial Risk, Policy and Controls at 202-586-6462.

**Distribution:**

Deputy Secretary  
Associate Deputy Secretary  
Chief of Staff  
Acting Under Secretary of Energy  
Under Secretary for Science  
Under Secretary for Nuclear Security/ Administrator for NNSA  
Assistant Secretary for Congressional and Intergovernmental Affairs  
Acting Assistant Secretary for Energy Efficiency and Renewable Energy  
Assistant Secretary for Environmental Management  
Acting Assistant Secretary for Fossil Energy  
Assistant Secretary for Nuclear Energy  
Assistant Secretary for Electricity Delivery and Energy Reliability  
Assistant Secretary for Policy and International Affairs  
Chief Information Officer  
Inspector General  
General Counsel  
Director, Office of Health, Safety, and Security  
Director, Office of Human Capital Management  
Director, Office of Indian Energy Policy & Programs  
Director, Office of Legacy Management  
Director, Loan Programs Office (LGPO and ATVM)  
Director, Office of Management  
Director, Office of Public Affairs  
Director, Office of Economic Impact and Diversity  
Director, Office of Hearings and Appeals  
Director, Office of Intelligence  
Director, Office of Budget  
Administrator, Energy Information Administration  
Power Marketing Administration Liaison Office  
Chairman, Federal Energy Regulatory Commission  
Manager, Chicago Office  
Manager, Idaho Operations Office  
Manager, Oak Ridge Office  
Manager, Richland Operations Office  
Manager, Savannah River Operations Office  
Manager, Golden Field Office  
Manager, Naval Reactors Laboratory Field Office  
Director, National Energy Technology Laboratory  
Project Manager, Strategic Petroleum Reserve Project Management Office  
Manager, EM Consolidated Business Center

**HO Resource Managers**

Director, Office of Resource Management, CI-3  
Deputy Director, Office of Management, Administration and Operations, IN-30  
Chief of Staff, Office of Economic Impact & Diversity, ED-1  
Chief Operating Officer, Office of Electricity Delivery & Energy Reliability, OE-1.1  
Director, Office of Planning, Budget Formulation & Analysis, EE-3B  
Director, Office of Resource Management & Information Services, EI-20

Deputy Assistant Secretary, Office of Policy, Planning & Budget, EM-10  
Director, Office of Executive Operations & Support, MA -1.1  
Associate Director, Office of Resource Management, SC-32.2  
Director, Office of Budget and Financial Management, FE-3  
Director, Administrative Operations, GC-90  
Director, Office of Field Financial Management, NA-MB-33  
Director, Office of Management Operations, HG-10  
Director, Office of Resource Management, PI-10  
Assistant IG, Office of Resource Management, IG-10  
Associate Director, Office of Resource Management, NE-1 0  
Director, Office of Resource Management, PA-3  
Director, Office of Resource Management, HS-1.2  
Director, Office of Program Management & Administration, RW-50  
Director, Office of Business Operations, LM -10  
Director, Office of Records and Business Management, IM-1 0  
Associate Administrator, Office of Management and Administration, NA-60

**Field Chief Financial Officers**

Chicago Office  
Idaho Operations Office  
Oak Ridge Office  
Richland Operations Office  
Savannah River Operations Office  
Golden Field Office  
Naval Reactors Laboratory Field Office  
National Energy Technology Laboratory  
Strategic Petroleum Reserve Project Management Office  
Bonneville Power Administration  
Western Area Power Administration  
Southeastern Power Administration  
Energy Finance and Accounting Service Center  
Southwestern Power Administration

U.S. DEPARTMENT OF ENERGY

# Internal Control Evaluations

---

Fiscal Year 2013 Guidance



Issued April 5, 2013

## Table of Contents

|  |    |
|--|----|
| <b>I. Introduction</b>   | 4  |
| A. Background  | 4  |
| B. Purpose   | 4  |
| C. Benefits of Performing Internal Controls Evaluations                  | 6  |
| <b>II. Important Dates</b>   | 6  |
| <i>Table 1: DOE Internal Controls Assessment Process Important Dates</i> | 7  |
| <b>III. GAO Standards for Internal Control in the Federal Government</b> | 7  |
| <b>IV. Focus Areas</b>   | 9  |
| <b>V. Importance of Risk Assessment in Internal Controls Evaluations</b> | 9  |
| A. The Risk Assessment Process   | 10 |
| B. Determining a Risk Response   | 11 |
| <b>VI. Evaluating Control Assessment Results</b>                         | 12 |
| <b>VII. Financial Management Assurance (FMA) Evaluation</b>              | 13 |
| A. FMA Evaluation Overview   | 13 |
| B. Financial Management Assurance (FMA) Tool                             | 14 |
| C. Scope of Evaluations  | 15 |
| D. Testing Requirements  | 17 |
| E. General Documentation Requirements                                    | 18 |
| <i>Table 3: Key Test Plan Elements</i>                                   | 18 |
| F. FMA Focus Area Guidance   | 19 |
| <b>VIII. Entity Evaluation</b>   | 20 |
| A. Four-Step Evaluation Process  | 22 |
| 1. Perform the Evaluation  | 22 |
| 2. Prepare and Track Corrective Action Plans (CAPs)                      | 23 |
| 3. Document the Evaluation   | 23 |
| 4. Report the Results  | 24 |
| B. Reporting on the Status of Management Priorities                      | 24 |
| <b>IX. Financial Management Systems (FMS) Evaluation</b>                 | 25 |
| <i>Table 4: DOE Financial Management Systems</i>                         | 25 |
| A. FMS Evaluation Process  | 25 |

|   |           |
|---|-----------|
| 1. Perform the Assessment .....   | 26        |
| 2. Prepare and Track CAPs .....   | 27        |
| 3. Document the Assessment .....  | 27        |
| 4. Report the Results.....  | 27        |
| <b>X. Mixed Systems Evaluation .....</b>  | <b>28</b> |
| <i>Table 5: DOE Mixed Systems</i> .....   | 28        |
| A. Mixed System Evaluation Process.....   | 28        |
| 1. Perform the Assessment .....   | 28        |
| 2. Prepare and Track CAPs .....   | 29        |
| 3. Document the Assessment .....  | 30        |
| 4. Report the Results.....  | 30        |
| <b>XI. Annual Assurance Memorandum .....</b>  | <b>30</b> |
| A. Reporting Documentation and Transmittal Methods .....  | 30        |
| <i>Table 6: Reporting Documentation Transmittal Methods</i> .....                                     | 31        |
| B. Format for the Assurance Memorandum .....  | 31        |
| C. Determining Issues to be Reported .....  | 31        |
| <i>Table 7: Definitions of Control Issues</i> .....   | 32        |
| <b><i>Table 8: Listing of Required Internal Control Evaluations by Departmental Element</i> .....</b> | <b>34</b> |
| <b>XII. Glossary .....</b>  | <b>35</b> |

# I. Introduction

## A. Background

In 1982, Congress enacted the [Federal Managers' Financial Integrity Act \(FMFIA\)](#), which requires each agency to establish and maintain [internal control](#) systems that allow obligations and costs to be recorded in compliance with applicable laws; funds, property and other assets to be safeguarded; and revenues and expenditures applicable to agency operations to be properly recorded and accounted for to permit the preparation of accounts and reliable financial information. Section II of [FMFIA](#) requires an assessment of non-financial controls to assure their effectiveness and efficiency and their compliance with laws and regulations. As a result, the Government Accountability Office (GAO) issued *Standards for Internal Control in the Federal Government* in order to provide a general framework for agencies to follow in designing their financial and non-financial internal control programs.

Following the publication of the GAO Standards, the Office of Management and Budget (OMB) issued [Circular A-123, Management's Responsibility for Internal Control](#), to provide specific guidance for agencies to follow in implementing internal control programs. In 1995, OMB revised Circular A-123 to require internal controls to support the purpose of the newly enacted *Government Performance and Results Act of 1993*, namely the improvement of program effectiveness and accountability. This revision required agencies to transmit a single annual [Statement of Assurance](#) from the head of the agency to the President, Congress, and OMB, stating whether there is reasonable assurance that the agency's controls are achieving intended objectives.

*The Public Company Accounting Reform and Investor Protection Act of 2002* (also known as Section 404 of the *Sarbanes-Oxley Act*) requires the management of public companies to assess and report on their companies' internal controls over financial reporting. In 2004, OMB revised Circular A-123 to hold federal managers to the same standards. Appendix A of revised OMB Circular A-123 requires federal managers to specifically assess and report on the agency's internal controls over financial reporting.

Circular A-123 defines internal control as the steps an agency takes to provide reasonable assurance that the agency's objectives are achieved through (1) effective and efficient operations, (2) reliable financial reporting, and (3) compliance with applicable laws and regulations. The safeguarding of assets is a subset of all of these objectives. Internal controls should be designed to provide reasonable assurance to prevent or detect unauthorized acquisition, use, and disposition of assets.

In October 2008, the Department of Energy (DOE) issued DOE Order 413.1B, *Internal Control Program*. Incorporating the requirements set out in the above-mentioned laws and regulations, this order requires "heads of [Departmental elements](#)... [to] evaluate and annually report on the adequacy of their organization's internal controls, including internal controls over financial reporting and if applicable, financial management systems." This guidance is intended to provide the specific methodology that reporting entities (including contractors) should follow to meet the requirements specified in Order 413.1B. Contractors required to follow this guidance are contractors with management and operating contracts that include the contract clause at DEAR 970.5204-2, *Laws, Regulations, and DOE Directives*.

## B. Purpose

DOE management is responsible for establishing and maintaining effective internal controls and [financial management systems](#) that meet the objectives of FMFIA and revised OMB Circular A-123, which provides guidance for the execution of FMFIA. In accordance with FMFIA requirements and DOE Order

413.1B, DOE management is responsible for establishing an internal control program and annually evaluating internal controls and reporting on the status of any identified [material weaknesses](#) up through the chain of command to the President, Congress, and OMB. These responsibilities also require management to implement a thorough Quality Assurance (QA) program to ensure the consistent application of DOE internal control standards and to provide insight to federal managers on the accuracy of the data that is reported through the controls assessment and reporting tools. To support Departmental reporting, heads of [Departmental elements](#) are required to report on the status of their organizations' internal controls, including [reportable conditions](#) identified and progress made in correcting prior reportable conditions.

In order to comply with the requirements in FMFIA and OMB Circular A-123, all Departmental elements are required to perform one or more of the following types of internal controls assessments:

- [Financial Management Assurance \(FMA\) Evaluation](#) (including specific consideration of activities funded by the American Recovery & Reinvestment Act (ARRA));
- [Entity Evaluation](#);
- [Financial Management Systems \(FMS\) Evaluation](#); and
- [Mixed System Evaluation](#).

The FMS Evaluation is required of select Departmental elements under the requirements as prescribed by the Federal Financial Management Improvement Act of 1996 (FFMIA) and OMB Circular A-127, which provides guidance for compliance with FFMIA. See [Table 8](#) of this guidance for a full listing of required assessments for each Departmental element.

In addition, all Departmental elements are required to maintain written policies and procedures for implementing the internal controls evaluations process described in this guidance. These policies and procedures must include the quality assurance (QA) program to be conducted by DOE field offices on submissions by their respective labs for the quality and accuracy of the content.

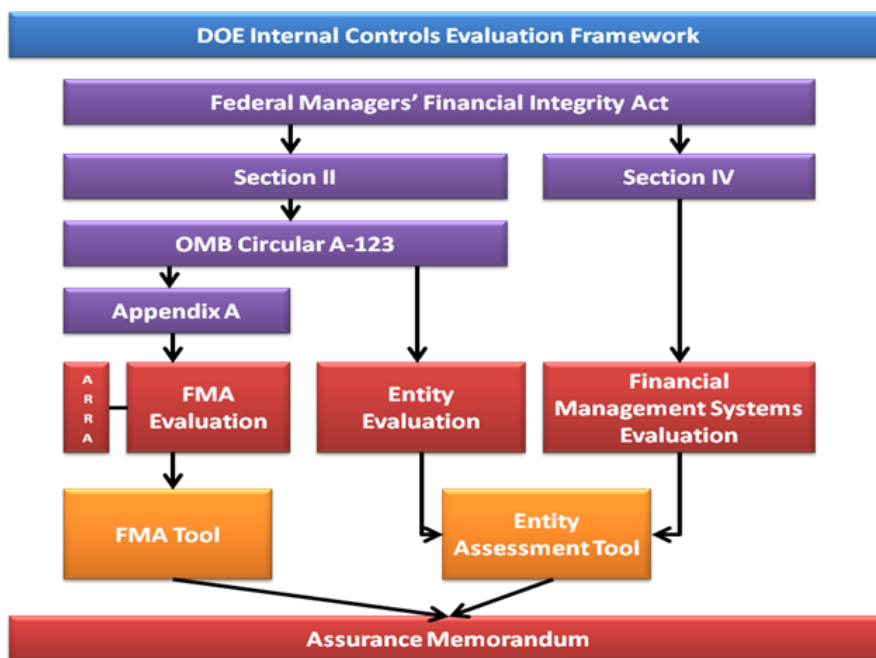
Management for each Departmental element should complete the QA validation before the submission of quality assurance results to the Office of Financial Risk, Policy, and Controls (CF-50). Senior management is responsible for ensuring that risk assessments, testing plans, sample sizes, and documentation of final results are compliant with DOE guidance. Departmental elements should establish and document their QA process and results. The QA process includes an assessment of the contractor internal control procedures and results by the cognizant Federal CFO office.

At the conclusion of the evaluation process, each Departmental element will summarize the results of their internal controls evaluations in their annual [Assurance Memorandum](#). Through the Assurance Memorandum, the head of each Departmental element provides reasonable assurance that financial and entity internal controls are working effectively and efficiently, financial reporting is accurate, and that operations were maintained in a manner consistent with applicable laws and regulations. Exceptions to such an assurance are reported as [reportable conditions](#), [material weaknesses](#), [material non-conformances](#), or [scope limitations](#). All field offices submit their Assurance Memoranda to the appropriate lead program secretarial office. Headquarters offices, considering any information submitted by their field offices, submit their Assurance Memoranda, addressed to the Secretary and to the Office of the Chief Financial Officer (OCFO). OCFO, in conjunction with the Departmental Internal Control and Audit Review Council (DICARC), assesses the assurances made from all the Departmental elements and provide the Secretary with a recommendation to sign the agency's [Statement of](#)

[Assurance](#). The final Statement of Assurance from the Department is then published in the Agency Financial Report and transmitted to the President, Congress, and OMB.

The framework for the DOE Internal Controls Evaluation process for each Departmental element, with its legal and regulatory underpinnings, is summarized in Figure 1 below.

Figure 1: DOE Internal Controls Evaluation Framework



### C. Benefits of Performing Internal Controls Evaluations

Ongoing evaluation of internal controls can provide significant benefits to all Departmental elements. Controls are designed to help [mitigate](#) risks. Thus, a controls assessment can show how well risk mitigation strategies are working and which strategies may need to be modified and improved. Ultimately, controls assessments serve as a tool that management can use to gauge the performance of a mission-based area. They can be tailored to show a macro perspective of an entire Departmental element as a whole, or to drill down into specific functions and processes. Performing controls assessments can allow managers to gain insight into the effectiveness of their programs and can lead to substantive improvements and best practices in mission execution.

## II. Important Dates

Table 1 below lists important dates in the Internal Controls Evaluation process. This includes deadlines for quarterly and annual reporting requirements. Submission of the FMA Tool for the first quarter of FY13 is not required. Management quality assurance reviews need to be completed prior to the quarterly and annual reports.

Table 1: DOE Internal Controls Assessment Process Important Dates

| Date              | Description  |
|-------------------|--|
| April 15, 2013    | Upload second quarter FMA Tool and FMA Quality Assurance Report to Internal Controls iPortal Space.  |
| April 15, 2013    | Entity status update (teleconference) to discuss any known preliminary issues in high risk areas or focus areas (see <a href="#">Section XI</a> ).   |
| June 28, 2013     | <a href="#">Departmental elements</a> performing FMA Evaluations complete testing of all High Combined risks identified in the current year assessment scope of the FMA Tool.              |
| June 28, 2013     | Departmental elements performing FMA Evaluations complete corrective actions and re-testing of all controls in remediation which may have a negative impact on the Statement of Assurance. |
| July 15, 2013     | Upload third quarter FMA Tool and <a href="#">FMA Quality Assurance Report</a> to Internal Controls iPortal Space.   |
| July 15, 2013     | Field offices and Power Marketing Administrations upload Entity Assessment Tool to Internal Controls iPortal Space   |
| August 2, 2013    | Field offices and Power Marketing Administrations upload Assurance Memorandum to Internal Controls iPortal Space.  |
| August 16, 2013   | Headquarters offices upload Entity Assessment Tool to Internal Controls iPortal Space.   |
| September 3, 2013 | Headquarters offices upload signed copies of the Assurance Memorandum to Internal Controls iPortal Space.  |

### III. GAO Standards for Internal Control in the Federal Government

Following the publication of [OMB Circular A-123](#), the GAO issued *Standards for Internal Control in the Federal Government*. This document outlines a framework for federal agencies to follow in establishing their [internal control](#) programs. In this framework, GAO identifies five standards that “define the minimum level of quality acceptable for internal control in government and provide the basis against which internal control is to be evaluated. These standards apply to all aspects of an agency’s operations: programmatic, financial, and compliance.”<sup>1</sup>

Below is a summary of the five GAO standards as published in OMB Circular A-123:

#### 1. Control Environment

The control environment consists of the organizational structure and culture created by management and sustained by employees that provides organizational support for effective internal control. The assessment should include obtaining a sufficient knowledge of the control environment to understand management’s attitude, awareness, and actions concerning the control environment. The assessment should consider the collective effect on the control environment, since management’s strengths and weaknesses can have a pervasive effect on internal control. Specific elements of the control environment that should be considered include:

- integrity and ethical standards;

<sup>1</sup>*Standards for Internal Control in the Federal Government*, Government Accountability Office, GAO/AIMD-00-21.3.1, 1999.

- commitment to competence;
- management philosophy and operating style;
- organizational structure;
- assignment of authority and responsibility; and/or
- human resources policies and practices.

## **2. Risk Assessment**

Risk assessment is the process by which management identifies internal and external risk that may prevent the Departmental element from meeting its mission objectives. The assessment should determine how management identifies risks, estimates the significance of risks, assesses the existence of risks in the current environment, and relates them to operations. The assessment should include obtaining sufficient knowledge of the agency's process on how management considers risks relevant to mission objectives and decides about actions to address those risks. The results of this assessment at the [Departmental element](#)-level will drive the extent of testing and review performed of internal controls. Some significant circumstances or events that can affect risk include:

- complexity or magnitude of programs, operations;
- extent of manual processes or applications;
- changes in operating environment;
- new personnel or significant personnel changes;
- new or revamped information systems;
- significant new or changed programs or operations;
- new technology; and/or
- new or amended laws or regulations.

## **3. Control Activities**

Control activities are the mechanisms that help ensure that management directives are carried out, mission objectives are met, and risks are effectively mitigated. The assessment should include obtaining an understanding of the control activities applicable at the Departmental element-level, such as:

- policies and procedures;
- management objectives (clearly written and communicated throughout the agency);
- planning and reporting systems;
- analytical review and analysis;
- segregation of duties;
- safeguarding of assets; and/or
- physical and access controls.

## **4. Information and Communication**

Relevant, reliable, and timely information should be communicated within the organization to relevant personnel at all levels and externally to outside stakeholders. The assessment should include obtaining an understanding of the information system(s) relevant to performance of mission objectives. Such an understanding should include:

- the type and sufficiency of reporting produced;
- the manner in which information systems development is managed;
- disaster recovery;

- communication of employees' control-related duties and responsibilities; and/or
- how incoming external communication is handled.

## 5. Monitoring

The effectiveness of internal controls should be monitored during the normal course of business. The assessment should include obtaining an understanding of the major types of activities the Departmental element uses to monitor internal controls, including the source of the information related to those activities and how those activities are used to initiate corrective actions. Several examples include:

- self-assessments by managers;
- periodic reviews, reconciliations, or comparisons of data;
- evaluation by the IG or external auditor; and/or
- direct testing.

## IV. Focus Areas

The Department annually identifies focus areas for the Financial Management Assurance (FMA) evaluation and Entity Evaluation processes. These focus areas represent areas of emphasis that require additional assessment. The focus areas are derived from repeat audit findings or areas of high risk within the Department. Additional focus area guidance is contained in [Sections VII.F.](#) and [VIII.](#)

## V. Importance of Risk Assessment in Internal Controls Evaluations

Accurate assessments of both financial and non-financial risks are integral to performing effective internal controls evaluations. Management should use risk assessments to identify which areas in the organization pose the highest threat to mission achievement if controls are not in place and functioning properly. In the passage below, GAO describes the responsibility of management to assess risk as part of maintaining adequate internal control.

Internal control should provide for an assessment of the risks the agency faces from both internal and external sources. Once risks have been identified, they should be analyzed for their possible effect. Management then has to formulate an approach for risk management and decide upon the internal control activities required to mitigate those risks and achieve the internal control objectives of efficient and effective operations, reliable financial reporting, and compliance with laws and regulations.<sup>2</sup>

As a result of a material weakness in safeguards and security, and other significant weaknesses and reportable conditions reported in recent years on non-financial controls, thorough risks assessments should be performed throughout the fiscal year for both financial and non-financial risks.

---

<sup>2</sup> *Internal Control Management and Evaluation Tool*, Government Accountability Office, GAO-01-008G, 2001.

## A. The Risk Assessment Process

Risks are assessed in a three-step process, which includes: (1) risk identification, (2) risk rating and (3) risk ranking. Risk assessment is iterative, and should be performed at regular intervals, or incorporated into existing processes, such as recurring program or project reviews.

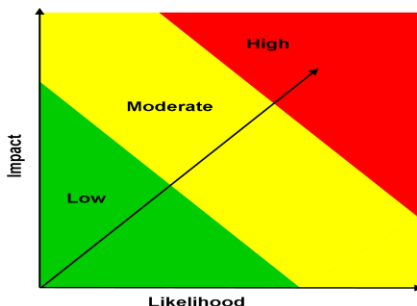
### 1. Risk Identification

An organization must define its mission-based objectives before conducting a risk assessment. Following this, the organization can identify the primary risks facing each of those objectives. In addition, risks can be identified by considering one or more of the following: key business processes and sub-processes; cross-cutting functions, such as budgeting, human resources, information management, or contract management; or risks pertaining to specific organizational units. Both financial and non-financial risks must be considered during the process. The organization should also consider both internal and external factors. Once identified, risks should be stated in an “if, then” or “cause and effect” format. The following are examples of common risks within DOE:

- Human Resources - *If the program does not have a sufficient number of qualified staff and managers available to effectively manage, oversee, and close out its projects, then project or program objectives will not be met.*
- Contractor Oversight - *If federal staff is unable to manage issues with contractor or awardee performance, such as performance or quality shortcomings, cost or schedule overruns, or non-compliance with laws and regulations, then waste, or abuse of government funds may occur and program objectives will not be met.*
- Acquisition and/or Procurement - *If a system is not in place to ensure competitiveness and fairness in contractor or awardee selection, then conflicts of interest may result.*
- Budget Execution - *If the organization does not follow established policies and procedures for budget execution, then government funds may be wasted, anti-deficiency violations may occur, and information regarding obligations, disbursements and outlays may be inaccurate.*
- Safeguards and Security - *If security procedures are not fully documented, supported by training for the appropriate personnel, and followed, then non-compliance with security requirements could occur and DOE property could be damaged or stolen or employee or public safety could be at risk.*

### 2. Risk Rating

In rating risks, management determines the likelihood of occurrence and the impact a risk would have on the organization, if it were to occur. Likelihood and impact are typically considered on a Low to High scale as shown below:



**Likelihood:** The measure of the relative potential that the risk might occur given the operating environment.

**Impact:** The measure of the magnitude and nature of the effect the risk might cause given the operating environment.

Initially, the likelihood and impact should be established assuming no controls are in place. This is referred to as the inherent or “exposure risk” rating.

Following the establishment of controls, risks are again rated, with consideration to the control environment. This latter risk rating should carry the greatest weight, as it reflects the organization’s “real-life” operating environment. At a minimum, an annual reassessment of risk ratings should be performed.

### **3. Risk Ranking**

Ranking risks helps to prioritize management’s attention to and decisions on the control environment. Risk rankings can be driven by measures of management concern, for example, the dollars exposed, potential reputational damage, the anticipated cost to remediate an event, if the risk was to occur, or the immediacy of the timeframe in which the risk could occur. For example, if a risk were to impact near-term mission objectives, then management may prioritize that risk in its rankings.

When ranking risks, management should first consider those risks that were rated “high” or “moderate”, in context of these additional measures of concern. Those risks that management ranks highest, are typically the risks that management will choose to mitigate first.

## **B. Determining a Risk Response**

After risks are assessed, management can then determine its risk response. Management should have a clear concept of its level of risk tolerance when determining what actions it will take to manage those risks that pose the greatest threat to achieving organizational objectives. For example, if management establishes a performance objective of 100%, is it willing to accept a result of 90%? Once its level of risk tolerance is set, management can choose its preferred risk response – to accept, avoid, reduce, share or transfer a risk. In selecting its risk response, management should give consideration to the current operating environment, including what existing processes can be leveraged to manage certain risks.

Establishing controls to manage risk is a common risk response. Typically, controls are put into place when the choice is to reduce or share a risk. Controls also may be implemented to avoid a risk. Management should keep in mind that controls can provide only reasonable assurance – not absolute assurance – that the risks will be mitigated. The risk that remains, or residual risk, should be within levels acceptable to management.

### **Using Controls to Manage Risk**

The determination of risk drives two major factors in the internal control process: (1) the placement of controls and (2) the prioritization of controls testing. The design and placement of controls is determined by the nature and severity of the risks identified in each process. Those controls must then be assessed to ensure they are functioning properly and effectively. Areas where risk is deemed highest may require a strengthening of existing controls or additional controls to be put in place. If, in the evaluation process, one finds that an area of high risk has insufficient controls to adequately mitigate

the risk, management should consider redesigning the existing controls. Alternatively, management can consider implementing additional controls. When determining the need for additional controls in high risk areas, managers must balance the cost of implementing an additional control with the benefit that control will bring in terms of added risk mitigation. There will be some areas in the high risk category that are inherently risky. The placement of additional controls may not result in greater mitigation in such instances.

### **Integration of Risk Assessments in Internal Controls Evaluations**

Risk assessments should be part of each Departmental element's process for developing internal controls and conducting the FMA Evaluation, Entity Evaluation, and FMS Evaluation. While the FMA Tool provides a direct and standardized approach for conducting risk assessments for the FMA Evaluation, a variety of approaches and templates can be used to conduct similar risk assessments as part of the Entity and FMS Evaluations. While it is expected that a determination of risk plays a key role in the internal controls evaluation process for each Departmental element, the results of those risk assessments are not required to be submitted with the Assurance Memorandum or the EAT and FMA Tool.

Documentation of the financial and non-financial risk assessments for each Departmental element should be maintained locally and is not part of the required documentation to be submitted to the Office of the Chief Financial Officer, except as part of the documentation required for the [FMA Tool](#), as discussed in [Section VII.B](#).

### **Risk Assessments Inform Controls Assessments**

Once a risk assessment is performed, management must assess and evaluate its financial and non-financial internal controls to assure that the control activities being used are effective and updated when necessary, by conducting a controls assessment. A control assessment is a formal review of the processes and controls associated with a specific or set of risk(s) to evaluate their effectiveness. A control assessment is a component of the overall internal controls evaluation process.

Generally speaking, sound business practices would dictate that not all controls are tested every year except in instances of previously reported significant deficiencies and material weaknesses. Risk assessments help to determine the frequency with which controls are tested. Controls in areas that have the highest risk should be tested more often than controls in areas that pose lower risk. In a three-year test cycle, for example, controls in high risk areas should be tested annually, while those in moderate risk areas are tested biannually and those in low risk areas are only tested once every three years. For example, see required test cycle for FMA Evaluations in See Section VII.C, [Table 2](#), FMA Evaluation Test Cycles. Previously reported significant deficiencies and material weaknesses should be tested each year until the controls are no longer deficient.

## **VI. Evaluating Control Assessment Results**

As discussed in the CFO Council Guide section on evaluating test results, test results should support management's judgment whether a control is functioning adequately. Exceptions noted in the testing of properly designed internal controls could indicate ineffectiveness. Management must consider the extent of a deficiency in such cases. Deficiencies can range from a *simple deficiency* (e.g., missing initials indicating a supervisor's review on 1 of 26 reconciliations sampled) to a *significant deficiency* (e.g., only 8 monthly reconciliations were performed for the year) and resulted in a loss of resources, to a *material*

*weakness* (e.g., reconciliation of several key accounts were not performed throughout the year) and resulted in a major loss of resources and breaches in security. A simple deficiency is an internal control deficiency that creates minimal exposure for management and is generally considered an anomaly. A significant deficiency usually indicates a history of internal control deficiencies that, when consolidated, equate to a reportable condition or material weakness. When exceptions are noted, management should assess whether the sample size should be expanded to validate whether an exception that appears to be a simple deficiency, is indeed an anomaly.

Regardless of the acceptable threshold established by management and the number of exceptions noted in testing internal controls, management needs to assess the exposure that **any** exception creates for the organization to determine the results. For example, with high-risk processes, one exception could have a significant impact on the organization, and therefore, needs to be assessed to determine if one failure should be reported as a material weakness.

The following sections discuss the specific controls assessment processes applied at the Department.

## VII. Financial Management Assurance (FMA) Evaluation

### A. FMA Evaluation Overview

There are five basic steps in performing the assessment of the effectiveness of [internal controls](#) over financial reporting. They are:

- Step 1: Planning;
- Step 2: Evaluating Internal Control at the Entity Level;
- Step 3: Evaluating Internal Control at the Process Level;
- Step 4: Testing Control Design and Operating Effectiveness at the Transaction Level; and
- Step 5: Concluding, Remediation, and Reporting.

Management's quality assurance program and related validation should encompass all of the above steps.

#### **Step 1: Planning**

Before beginning an evaluation, a certain amount of planning is required. Each reporting entity should review all of the processes and sub-processes applicable to their functions. Detailed steps for these processes and how they interact, as well as the controls put in place to mitigate known risks within those processes, should be diagrammed in a process map. Changes in any processes should be identified and the process map should be updated. In addition to updating the process maps, reporting entities should review all of the current controls in place within these processes to determine if their design is still adequate to address the risks they are mitigating.

#### **Step 2: Evaluating Internal Control at the Entity Level**

The process to execute this step is described in [Section VIII](#) of this guidance.

#### **Step 3: Evaluating Internal Control at the Process Level and Step 4: Testing Control Design and Operating Effectiveness at the Transactional Level**

The processes to execute these steps are described in the remainder of this section. This includes performing quality control on the content input into the FMA Tool by running the Quality Assurance Tool ([QA Tool](#)).

#### **Step 5: Concluding, Remediation, and Reporting**

The processes for executing this step are described in [Section VII.E](#) and [Section XI](#) of this guidance.

Documentation occurs within each of the basic steps outlined above, whether documenting the evaluation methodology during the planning step or documenting key processes and test results during the evaluation and testing steps.

### **B. Financial Management Assurance (FMA) Tool**

The [FMA Tool](#) serves as the primary central repository for documenting the relevant processes, sub-processes, and risks facing each reporting entity, as well as the [key controls](#) for each process that are relied upon to [mitigate](#) risks. Reporting entities are not required to prepare supplemental documentation specifically to support the [FMA Evaluation](#). However, reporting entities should reference in the FMA Tool the existing documents that support the identification of the controls and verification of the applicability of the standard process, sub-process, and corporate risks to the site. Such documents can take the form of process mapping.

Specifically, the following should be completed by all reporting entities that are required to perform an FMA Evaluation (see [Table 8](#) for a detailed list):

1. Localize the FMA Tool by selecting the relevant [Departmental element](#).
2. All [standard processes](#) and [sub-processes](#) (those pre-populated in the FMA Tool) applicable to the reporting entity should be selected in the FMA Tool.
3. The FMA Tool automatically populates all [corporate risks](#) associated with the sub-processes selected in step 1. Add any local risks specific to the reporting entity into the FMA Tool.
4. For the selected standard processes and sub-processes, corporate risks should be evaluated for applicability and those that are not applicable should be annotated by selecting “NR” in the Exposure column (which will gray out that risk line).

Reporting entities are required to document the rationale for risks assessed to have an exposure rating of NR or Low.

5. In the Risk Assessment section of the tool, an [assessment of exposure](#) for each identified risk should be conducted, assuming no controls are in place, and the appropriate rating (i.e., not rated (NR), low, moderate, or high) should be input in the tool. Exposure risk ratings are based on the likelihood of the risk occurring and the impact on the reporting entity if the risk does occur, in the absence of controls. A heat map explaining the determination of exposure risk can be found in [Section XII](#).

Re-evaluate all prior exposure ratings against the [risk factors](#) in the tool. Risk factors are changes that may affect the exposure risk or effectiveness of the existing controls in

mitigating the risk. These include system changes, process changes, organization changes, other changes (i.e., audit, IG, GAO, etc.).

6. Assess the [control risk](#) (also known as [dual-purpose testing](#)) for each risk identified in the tool. The control risk is a calculated field in the tool based on [Risk Occurrence](#) and [Control Set Execution](#).
  - a. **Risk Occurrence:** Determined during dual-purpose testing. Ask, did the risk occur during normal business operation?
    - i. **1** – No occurrence;
    - ii. **2** – Risk occurred within acceptable threshold; or
    - iii. **3** – Risk occurred outside the acceptable threshold.
  - b. **Control Set Execution:** Rating based on assessment testing results of all individual controls within a control set.
    - i. **1** – Passed with no failures;
    - ii. **2** – Passed with failures within acceptable threshold; or
    - iii. **3** – Failed.
  - c. A graph combining risk occurrence ratings and control set execution ratings to determine the control risk can be found in [Section XII](#).
7. Based on the risk exposure rating and the control risk rating, the [combined risk](#) rating for each identified risk is automatically calculated. A graph showing how combined risk ratings are determined can be found in [Section XII](#).
8. Controls must be identified for any risks meeting the [minimum evaluation standard](#) in the combined risk category. Controls for risks with a combined risk rating of High must be tested each year. Controls with a combined risk rating of moderate must be tested at least every two years. Controls with a combined risk rating of Low must be tested at least every three years. Controls do not need to be identified for risks with an exposure risk rating of Low in the tool.
9. Complete summary information for each [Corrective Action Plan \(CAP\)](#) required as a result of testing in the CAP Tracking Tab.
10. Run the [FMA Quality Assurance \(QA\) Tool](#) to ensure that all fields have been completed properly. The resulting QA report must be submitted along with the FMA Tool. Management for each Departmental element should resolve QA Tool exceptions before the submission of QA Tool results to the Office of Financial Risk, Policy, and Controls (CF-50). The QA Tool is only a portion of the QA program and senior management is also responsible for ensuring that risk assessments, testing plans, sample sizes, and final results are compliant with DOE guidance. Departmental elements should establish and document their QA process and results.

### C. Scope of Evaluations

Below is a table of the risk-based test cycles that govern the scope of the FMA Evaluation. Note that the combined risk rating is calculated based on the [exposure risk](#) rating and the [control risk](#) rating.

Table 2: FMA Evaluation Test Cycles

| Risk Ratings  |  |                 | Test Cycle             |
|---------------|--|-----------------|------------------------|
| Exposure Risk | + Control Risk   | = Combined Risk |                        |
| High          | High or Moderate   | High            | Annual (every year)    |
| High          | Low  | Moderate        | At least every 2 years |
| Moderate      | High or Moderate   |                 |                        |
| Moderate      | Low  | Low             | At least every 3 years |
| Low           | Specific testing for FMA not required. However, reporting entities are individually accountable for ensuring that Low risks are managed and that related controls are functioning using the most effective/efficient method deemed reasonable. Management decisions on how to manage Low risks should be documented. |                 |                        |

**Risk Factors:** Risks should be re-assessed annually. Each Departmental element should consider whether risk factors, such as organizational restructurings, system changes or upgrades, process changes, audit findings, or other changes would impact its risk ratings. If so, the controls related to those risks should be evaluated in the current year. In the FMA Tool, new or changing risk factors modify the Combined Risk to “UKN” (unknown) and require further analysis and/or retesting in the current year.

In FY 2013, Departmental elements are expected to perform the steps outlined below.

1. Follow the risk-based test cycles described in Table 2 above and complete testing of all controls for processes that have risks with a combined risk rating of High as identified in the current year assessment scope by the FMA Tool, no later than June 28, 2013. Also complete testing of controls for processes that have risks with a combined risk rating of Moderate that were identified last year and not tested (as per the two-year testing cycle described above).
2. Complete testing of any controls for processes that have risks with an exposure risk rating of High that have not been previously tested and do not yet have a risk rating in the Combined category (i.e., new risks identified this year, items whose prior year exposure rating has been raised from low or moderate to high, recently remediated items, etc.).
3. Complete corrective actions and re-testing of all controls in remediation (i.e., those controls that exceed established test failure thresholds) by June 28, 2013, which might have a negative impact on the Assurance Memorandum (i.e., cause a qualification of the Assurance Memorandum) if not corrected by that date. A [Corrective Action Plan \(CAP\)](#) should be developed for each area of remediation. The CAP should be a detailed, step-by-step plan with associated milestones. Each CAP should also contain the signatures of the authorized individual approving the plan and the individual confirming completion of the plan.

While there is not a prescribed format for a CAP, it should contain the key elements listed below. The significant information should be summarized in the CAP-Track tab of the FMA Tool. Departmental elements will maintain the CAPs and will not be required to submit the CAPs unless requested by the OCFO.

- summary of the [control deficiency](#);
- summary of [remediation activities](#);
- process/sub-processes affected;
- date identified;

- exposure and combined risk assessment;
  - remediation target (e.g., training, system, organization, etc.);
  - accountable individual; and
  - status.
4. Complete required actions to address all FY 2013 [focus areas](#) and document the actions taken in the focus area tab of the FMA Tool. Annually, the OCFO identifies focus areas for its FMA Evaluation areas of emphasis. These focus areas must be tested within the assessment year (if exposure risk is rated moderate or high). [Section VII.F](#) provides additional information on focus areas and specific requirements for assessing these areas.
  5. If, during the course of testing, any best practices are identified for improved control effectiveness, efficiency, or monitoring, they should be denoted in the Assessment Tab of the FMA Tool as “efficiency opportunities.” Departmental elements are encouraged to document those best practices and share them with the appropriate departmental element, where applicable. These best practices will be shared with other Departmental elements, in order to facilitate control improvements agency-wide.

## D. Testing Requirements

There are a variety of different techniques available to test internal controls. Below are just a few that may be considered in conducting tests of internal controls.

- Interviews, which can be either in-person or through the use of questionnaires. In general, it is considered a best practice to have information gathered from interviews be corroborated with a secondary type of evidence. However, this may not always be possible.
- Direct observation of performance of the control.
- Physical examination or inspection of documents.
- Transaction testing and re-performance, the latter being most commonly used when testing automated controls.

Organizations may employ a variety of evaluation activities and consider a wide-range of reliable existing information to effectively test internal controls. Examples of typical activities and considerations that may be used include, but are not limited to:

- Departmental Management Priorities;<sup>3</sup>
- consideration of the results of Inspector General (IG) and GAO audit reports (required in all cases);
- review of prior-year Assurance Memoranda and EAT and FMA Tool submissions;
- review and analysis of existing “Assurance System” reports/results;
- consideration of contractor and site office internal controls evaluation reporting (provided to Lead Program and Cognizant Secretarial Offices prior to year-end reporting);
- review and analysis of performance reporting results;
- consideration of the results of other internal or external assessments;
- conduct of management meetings and/or interviews with critical staff regarding key control areas;

---

<sup>3</sup> Complete summaries of the Management Priorities can be found in the FY 2012 Agency Financial Report: <http://www.cfo.doe.gov/cf12/2012PARafr.pdf>.

- review of relevant management reports (i.e., safety manager reports, infrastructure status reports, etc.); and/or
- review/analysis of other relevant and reliable information.

Reporting entities must use dual-purpose testing where applicable. Dual-purpose testing is designed to evaluate both control execution (i.e., did the control operate as intended) and risk occurrence (i.e., is there evidence that the stated risk occurred). Dual-purpose testing is important because it provides a mechanism for ensuring that controls are actually effective in risk mitigation, thereby reinforcing the site's control design effectiveness decision. Test plans should clearly convey this type of dual-purpose testing, recognizing that in some cases control execution and risk occurrence are tested simultaneously.

In testing control activities, reporting entities should use the guidelines outlined below when selecting testing samples:

1. Use professional judgment in determining appropriate sample sizes for testing.
2. Sample sizes should be selected considering the:
  - a. combined risk rating;
  - b. sample universe; and
  - c. control attributes (e.g., frequency, mode, type, etc.).
3. Reporting entities should use the OMB and CFO Council Guide sample size guidelines presented in Figure 2.

*Figure 2: Sample Sizes*

After considering the complexity of a control, the following are examples of sample sizes based on the frequency of the performance of the control:

|                                       |                                     |
|---------------------------------------|-------------------------------------|
| performed annually – sample size = 1  | performed weekly – sample size = 10 |
| performed quarterly – sample size = 2 | performed daily – sample size = 30  |
| performed monthly – sample size = 3   | recurring – sample size = 45        |

In addition, whether the control is manual or automated should also be considered. Ultimately, management should use its best judgment to determine how extensively a key control will be tested.

## E. General Documentation Requirements

In FY 2013, in addition to the control/process documentation requirements, reporting entities must also ensure the following activities are documented to support internal/external review or audit.

- [Exposure Risk Assessment](#) – **Must be rated** in the FMA Tool. Reporting entities must provide the rationale for all risks rated as “Low” or “NR” in the Exposure column. Reporting entities should record the justifications for those risks rated as moderate or high exposure to support a more effective re-evaluation of exposure on an on-going basis.
- [Testing Activities](#) – Test plans and results **must be documented** in a formal test plan containing the key elements outlined in Table 3 below. Testing results **must be updated** in the FMA Tool.

*Table 3: Key Test Plan Elements*

|                          |                         |
|--------------------------|-------------------------|
| Description of objective | Sample size             |
| Type of test             | Timeframes of execution |

|  |                        |
|--|------------------------|
| Procedures of the test being performed       | Resources assigned     |
| Acceptable error thresholds                  | Date executed          |
| Explanation of the extensiveness of tests    | Approver               |
| Universe from which sample size was selected | Who performed the test |

- [Remediation Activities](#) – Corrective Action Plans (CAPs) **must be maintained** and be readily available to support reviews or audits for all remediation activities identified in the FMA Tool. The FMA Tool **must also be updated** to summarize key remediation information required in the Assessment tab. In addition, a summary of all current and previously reported open reportable conditions and material weaknesses should be included in the Assurance Memorandum. Please see [Section XI](#) for explicit instructions on completing the Assurance Memorandum.
- [Best Practices](#) – Reporting entities should leverage the FMA Evaluation process to identify future improvements in efficiency, effectiveness, or monitoring. In addition, reporting entities may use the Efficiency column in the FMA Tool to note the potential best practice and briefly document the nature of the best practice for future use. Reporting entities are encouraged to share best practices with the OCFO in order to facilitate implementation of possible improvements agency-wide. Such activities should be pursued as time and resources permit; however, there are no specific requirements for adopting efficiency changes.

## F. FMA Focus Area Guidance

The Department’s FY 2013 FMA focus areas are managed through the “Focus Area” tab in the FMA Tool. This tab includes all corporate risks, with focus area risks highlighted with a “Y” in the Focus Area Column. In addition, for each focus area risk, the “Description/Action Required” column provides information on what actions are to be taken in FY 2013, as well as some insight into why a particular area was selected.

When a focus area is selected in the Focus Area tab (this is done through an import tool provided by the FMA Program Manager), the “Corp Request” column in the Assessment tab is highlighted with a yellow “Y” and the area shows up in the current year scope. Reporting entities should review and take the appropriate actions as indicated. Once actions are completed, the site should use the drop down to place a “Y” in the “Local Action Complete” column of the Focus Area tab. Then, the site should provide a brief description of the actions taken. Once this is done, the “Corp Request” column in the Assessment Tab will change to an “A” to indicate a focus area existed and site action was taken.

At every reporting entity, focus area actions should be taken if the exposure rating for these focus area risks is either high or moderate. If a focus area is rated as Low Exposure in the FMA Tool, check the “Y” under Local Action Taken and insert the following in the Action Taken column “Not Rated (NR) - Exposure Verified as Low”. Focus areas with a low exposure rating are not required to be tested in the current year. An NR rating may also be given if there is no activity related to that focus area risk. This risk rating should be validated as part of quality assurance activities.

**ARRA Focus Areas:** Reporting entities should review each ARRA focus area risk and determine if they have any relevant ARRA funding/activities related to the stated risk. The specific standard processes included as ARRA focus areas include Cost Management, Grants Administration, Acquisition Management, Payables Management, and Project Cost Management.

If relevant, the site should: a) Determine whether existing testing is within cycle and includes ARRA activities in the test sample; b) Determine if existing testing is adequate and, if so, no action is required – if not, re-test with ARRA activities in the sample and/or perform limited supplemental testing to cover ARRA activities; c) Check “Y” in the Local Actions Taken column and provide a description of actions taken (Note: If re-testing is performed, the test results in the FMA tool must be re-evaluated).

If not relevant, reporting entities should check “Y” in the Local Action Taken Column and record the following in the description of actions taken column – “No relevant ARRA activities for the site.”

In testing controls in standard processes included as ARRA focus areas, reporting entities should consider whether the requirements associated with ARRA funding have significantly changed the dynamics of the control environment or otherwise provided enhanced stressors to the controls previously tested. Key questions to help in making this determination include:

- Did the ARRA funding require use of more manual processes/controls?
- Did ARRA funding represent a significant increase in activity that may impact control operation or effectiveness, such as contract or grant monitoring or closeout?
- Did ARRA funding require use of different or increased personnel levels?
- Other questions deemed appropriate by the site.

If the answer is yes to any of these or other key questions developed by the site, then re-testing should be performed, even if controls for the risk were previously tested. If the answer is no to all questions, reporting entities should revert to the standard test cycle described in [Section VII.C](#) of this guidance. Reporting entities must also document the rationale for not re-testing in the Comments column of the FMA Tool.

**Control vs. Process Documentation:** Note that some actions require only that controls be documented (in the FMA Tool), while others specifically state that processes or other specific activities be documented (i.e., roles and responsibilities or a communications strategy). Please be sure that the specific required actions are performed. In cases where processes are requested to be documented, the site should prepare supplemental process narratives and/or flows, and maintain that documentation in a current status on an on-going basis.

**Process Documentation:** Process or other documentation required should be maintained locally. This documentation is critical for supporting the FY 2013 financial statement audit conducted by DOE’s external auditor. In addition, the process documentation for the focus areas will likely be requested for quality assurance/peer review purposes.

## VIII. Entity Evaluation

As in prior years, all [Departmental elements](#) are required to perform an evaluation, as shown in [Table 8](#), of the [internal controls](#) in place for non-financial functions (administrative, operational, and programmatic), collectively referred to throughout this guidance as entity functions. An [Entity Evaluation](#) is a structured self-evaluation designed to provide reasonable assurance that non-financial control systems are in place and working effectively to [mitigate](#) risk and ensure mission objectives are

accomplished effectively, efficiently, and in compliance with laws and regulations. This assessment may incorporate a variety of techniques to provide the required level of assurance. The results of the Entity Evaluation will be reported in the Departmental element's annual Assurance Memorandum to the Secretary, who in turn will report synthesized results for the entire agency to the President, Congress, and OMB through the [Statement of Assurance](#).

Section II of [FMFIA](#) requires an assessment of non-financial controls to assure their effectiveness and efficiency and their compliance with laws and regulations. There are several principles that can help guide each Departmental element's performance of the Entity Evaluation.

1. The purpose of internal controls evaluations is to test the effectiveness of controls already in place and identify gaps in internal controls.
2. Internal controls must be tested to determine if the controls are functioning effectively and performing their designated objectives.
3. The results of internal controls evaluations must be documented and retained to support the conclusions reached.
4. The results of internal controls evaluations provide the basis for the Department's Statement of Assurance, which is published in DOE's Agency Financial Report.
5. The monitoring of internal controls is an on-going process. Assessments of internal controls are not limited to an annual exercise and may be conducted multiple times per year, especially in areas that have high inherent risk or are central to mission fulfillment. While the head of the Departmental element is responsible for the direction and oversight of internal controls evaluations, the evaluations can be performed by other in-house or contractor personnel.
6. If significant [control deficiencies](#) or indications of potential weaknesses are identified, these issues must be reported.

### **Entity Focus Area Guidance**

Focus areas are identified in the EAT with a "Y" in the Focus Area column in the Entity Evaluation tab. Each Focus Area should be considered and reviewed based on the control objectives and considerations stated in the EAT. The Basis of Evaluation section of the EAT should reflect the results of controls assessments for each Focus Area, if applicable.

### **Entity-level Risk Assessments**

Risk assessments should be performed before beginning the entity control assessments. Entity-level risk assessments are performed by each Departmental element and documentation on these assessments must be retained locally.

As discussed in [Section V](#), entity-level risks should be assessed at least annually, and should focus on the key non-financial risks that would impact the organization's ability to meet its mission objectives. Risks should be identified, rated, and ranked, according to areas of management concern. Several examples of non-financial risks are provided in Section V.

### **Identifying Non-Financial Controls**

Assessments of entity-level, or non-financial controls are also performed by each Departmental element and documentation must be retained locally. The Entity Assessment Tool, which is submitted to the Office of Financial Risk, Policy and Controls, documents the outcome of local assessments of non-financial controls. When performing entity-level controls assessments, Departmental elements should consider the following types of controls:

- **Managerial** – reviews and checks that occur regularly as part of the oversight process, such as periodic project or program reviews
- **Program/Operational** – discrete activities related to program performance and effectiveness and efficiency of operations, such as mandatory training or cascading of organizational objectives through individual performance plans
- **Accounting** – activities that ensure safeguarding of assets, such as inventory management or physical security over valuable property (physical access controls, locks, guards)
- **Administrative** – activities related to the authorization of transactions or events that ensure compliance with existing policies and procedures, such as approval or certification actions, or establishment of role/responsibility controls in information management systems

## A. Four-Step Evaluation Process

The Entity Evaluation process has four steps:

1. **Perform the Evaluation:** Each Departmental element will be responsible for performing an Entity Evaluation to assess the effectiveness of its most critical entity internal controls for ensuring that mission objectives are met effectively, efficiently, and in compliance with applicable laws and regulations. Departmental elements should leverage existing resources and assurance activities to perform this assessment.
2. **Prepare and Track [Corrective Action Plans \(CAPs\)](#):** CAPs should be developed and tracked through completion for any control deficiencies identified.
3. **Document the Evaluation:** Each Departmental element will document the Entity Evaluation using the [Entity Assessment Tool \(EAT\)](#), which will be provided to all FMFIA points of contact to guide and substantiate the assessment and remediation process.
4. **Report the Results:** The results of the Entity Evaluation will be reported in an annual Assurance Memorandum.

### 1. Perform the Evaluation

The Entity Evaluation evaluates the Departmental element's controls against the five GAO Standards for Internal Control. The five standards are broken down into 22 key control areas that must be evaluated.

Departmental elements may elect to perform the Entity Evaluation using a variety of techniques; however, two basic tenets must be followed in any assessment. First, all assessments must touch on every aspect of the Departmental element. Second, all assessments should consider the five GAO Standards for Internal Control, described in [Section III](#) of this document.

### **Testing**

The breadth and depth of controls testing should be determined by the Departmental element's assessment of entity-level risks. Those areas where risks are moderate or high should have controls tested more often than those areas where risks are determined to be low. The nature and extent of activities employed in conducting an Entity Evaluation is at the discretion of each Departmental element. Controls identified during the assessment must be tested in order to determine if they:

- accomplish their objectives as designed;
- are necessary and sufficient to accomplish their intended objectives; and
- function appropriately.

In addition, reporting entities should consider establishing sample sizes and failure thresholds for each control being tested. It is important to determine in a test plan how many instances of a control activity will be tested and of those instances, how many failures of individual instances of the control activity constitute a failure of the entire control. Specific guidance on performing control tests, including guidance on sample sizes, is provided in [Section VII.D](#).

### **Leveraging Existing Assurance Activities**

FMFIA requires management to monitor the status of internal controls on an on-going basis and design control systems to address key risks. As such, Departmental elements should seek to leverage the results of existing assurance systems, such as the Contractor Assurance System, and other information, to the extent possible, to help evaluate the current status of controls. Where existing information/activities are not sufficient to validate the current status of controls, programs should identify and take additional steps to verify the status of the controls to ensure there is adequate support for the program's certifications in the annual Assurance Memorandum.

Departmental elements should perform additional evaluation/validation activities where relevant and reliable information is not available to be leveraged.

## **2. Prepare and Track Corrective Action Plans (CAPs)**

A CAP should be created and tracked internally for any control deficiencies identified through the internal controls assessment process. If management determines that any of these issues are of high enough materiality to warrant being reported as a [reportable condition](#) or [material weakness](#) in the Assurance Memorandum, a CAP Summary describing the status of [remediation activities](#) must be submitted with the Assurance Memorandum. CAP Summaries should be prepared using the "HQ Assurance Memo Template" or "Field Assurance Memo Template" provided in conjunction with this Guidance. Additional instructions for filling out the CAP Summary are provided in [Section XI](#). CAPs for reportable conditions and material weaknesses should be prepared and tracked locally. In addition, summary information for the CAP should be maintained in the EAT. Please refer to the EAT User Guide for detailed instructions on how to document CAPs in the EAT.

## **3. Document the Evaluation**

The EAT will be provided to your program's specific FMFIA point of contact to document critical information regarding your Entity Evaluation in a common format to support corporate consolidation and analysis. The completed EAT will be submitted two weeks in advance of the Assurance Memorandum and will serve as the primary source of documentation for the FMFIA Entity Evaluation.

The EAT will document the most critical supporting information including:

- the [basis of evaluation](#) for standardized key control areas;
- the results of the review;
- [impact assessments](#) for significant issues identified; and
- other critical information.

As such, it will not be necessary to maintain additional extensive documentation to support the assessment, assuming a thorough job is done in completing the EAT.

Reporting entities will not be required to keep copies of key documents leveraged for the evaluation in a central location. However, the location of the documents can be noted in the EAT and documents must

be readily available if requested during controls assessments and/or quality assurance reviews by Headquarters CFO staff, peer review teams, or internal and external auditors. FMFIA points of contact should maintain copies of documents that are not readily available and/or were prepared solely for the purpose of supporting the FMFIA process (e.g., FMFIA meeting minutes, special reviews performed for FMFIA purposes, etc.). Documentation beyond the EAT and the Assurance Memorandum should be maintained locally unless requested by the CFO, Inspector General, or peer review teams.

It is management's responsibility to ensure that the EAT comprehensively documents the results of the Entity Evaluation process. Management should perform a quality assurance review on the EAT before submission, to ensure that that risk assessments, testing plans, sample sizes, and final results are compliant with DOE guidance. Departmental elements should establish and document their QA process and results.

#### **4. Report the Results**

Results of the Entity Evaluation should be reported in the annual Assurance Memorandum. To determine what to report in the Assurance Memorandum, review all of the issues rated as a "1", "2", or "3" in the EAT. These issues are known as control deficiencies. Those deficiencies rated as a "2" or a "3" may rise to the level of a reportable condition if they are determined to significantly impact mission/mission support activities, effective/efficient operations, safety/security, and/or ability to meet critical commitments. Please note that all reportable conditions must be reported in the Departmental element's Assurance Memorandum and must have a CAP Summary attached to the Assurance Memorandum. In addition, all control deficiencies must be documented in the EAT.

Please see [Section XI](#) of this guidance for detailed instructions on how to compose and address the Assurance Memorandum. A macro-enabled template for the Assurance Memorandum is also available as a separate electronic attachment to this guidance. Please note that there are two Assurance Memorandum templates – one for field offices and one for headquarters offices. Please make sure to use the appropriate template.

### **B. Reporting on the Status of Management Priorities**

*(Management Priority Owners only):* The Department identified nine Management Priorities in its FY 2012 Agency Financial Report. These represent the most important strategic management issues facing the Department in accomplishing its mission. Departmental elements that are primarily responsible for these Management Priorities (priority owners) are required to provide quarterly updates to the priority summaries, including Departmental initiatives taken to date and those remaining to be completed. Increasing the frequency of reporting on Management Priorities provides for more complete and timely information to inform the Departmental Internal Control and Audit Review Council (DICARC) on areas requiring senior management attention. All Management Priorities must be submitted in the format of the existing Departmental Management Priorities as published in the Agency Financial Report. Specifically, priority owners will address key challenges and departmental initiatives (both those taken in the current fiscal year and initiatives to be undertaken in the future). Complete summaries of the Department's Management Priorities listed below can be found on the Internal Controls group space in iPortal.

- *Contract and Project Administration* (Priority Owner – Office of Management).
- *Acquisition Process Management* (Priority Owner – Office of Management).
- *Security* (Priority Owner – Office of Health, Safety and Security).
- *Environmental Cleanup* (Priority Owner – Office of Environmental Management).

- *Nuclear Waste Disposal* (Priority Owner – Office of General Counsel/Nuclear Energy).
- *Cyber Security* (Priority Owner – Office of Chief Information Officer).
- *Human Capital Management* (Priority Owner – Office of Chief Human Capital Officer).
- *Safety and Health* (Priority Owner – Office of Health, Safety and Security).
- *Recovery Act* (Priority Owner – American Recovery & Reinvestment Act Office).

Quarterly updates should be uploaded to the Internal Controls space on iPortal. Year-end updates must be included as part of the annual Assurance Memorandum.

## IX. Financial Management Systems (FMS) Evaluation

The [FMS Evaluation](#) must be performed annually by [Departmental elements](#) with [financial management systems](#) included in the DOE Financial Management System Inventory. This will support core requirements of Section IV of [FMFIA](#) and the Federal Financial Management Improvement Act (FFMIA). Only Departmental elements listed as system owners should perform the FMS Evaluation.

OMB Circular A-127, *Financial Management Systems*, defines a financial system as a “core financial system” that may perform all financial functions and is the system of record that maintains all transactions resulting from financial events. A “[mixed system](#)” is an information system that can support both financial and nonfinancial functions. A core financial system requires compliance with a greater set of criteria than a mixed system. For example, core financial systems are required to use the U.S. Standard General Ledger (USSGL) at the transaction level, but a mixed system is not required to use the USSGL. Table 4 below provides the applicable core financial systems inventory. Section X and Table 5 of this guidance provide the evaluation procedures for mixed systems.

Table 4: DOE Financial Management Systems

| Financial Management System                                     | System Owner(s)                    |
|---|------------------------------------|
| <b>Power Marketing Administration Systems</b>                   | <b>BPA, WAPA, SWPA, &amp; SEPA</b> |
| <b>iManage Standard Accounting and Reporting System (STARS)</b> | <b>CF-40</b>                       |
| <b>Federal Energy Regulatory Commission Systems</b>             | <b>FERC</b>                        |

In accordance with the FFMIA guidelines, system owners should determine whether the financial systems in Table 4 above conform to federal financial management systems requirements. FFMIA was intended to advance federal financial management by ensuring that federal financial management systems can and do provide reliable, consistent disclosure of financial data and that they do so on a basis that is uniform across the federal government from year-to-year, consistently using generally-accepted accounting principles.

### A. FMS Evaluation Process

The FMS Evaluation process generally follows the same four-step process used for the [Entity Evaluation](#), described in [Section VIII](#) of this guidance. These four steps are:

1. Perform the Assessment;
2. Prepare and Track [CAPs](#);
3. Document the Assessment; and

#### 4. Report the Results.

### 1. Perform the Assessment

FFMIA requires agencies to have financial management systems that substantially comply with the federal financial management systems requirements, standards promulgated by the Federal Accounting Standards Advisory Board (FASAB), and the U.S. Standard General Ledger (USSGL) at the transaction level. Financial management systems shall have general and application controls in place in order to support management decisions by providing timely and reliable data.

To meet these requirements, those Departmental elements that are designated as owners of the financial systems listed in Table 4 above must design and perform tests of those systems. These tests should be designed to evaluate the degree to which each system meets the criteria below.

1. System provides an agency-wide financial information classification structure that is consistent with the USSGL.
2. Financial management systems are adequately integrated.
3. System provides use of the USSGL at the transaction level.
4. System provides timely and useful reports on the financial information and performance measures.
5. System supports budget preparation, execution, and reporting in accordance with OMB.
6. System adheres to design, development, operation, and maintenance requirements.
7. System incorporates Government Information Security Reform Act and other government-wide computer security requirements.
8. System is supported by up-to-date system documentation adequate for user needs.
9. System contains appropriate internal controls.
10. Adequate system training and user support services are provided.
11. Ongoing maintenance of system is conducted for continued effective and efficient operations.
12. System supports adherence to federal accounting standards.

There are three common test techniques that can be implemented to perform the necessary tests required for an FMS Evaluation:

1. Direct observation of performance of the control.
2. Physical examination or inspection of documents.
3. Transaction testing and re-performance, the latter being most commonly used when testing automated controls.

In implementing the physical examination of documents test technique, managers should consider a variety of existing information at their disposal. Examples of such sources of information are:

- results of external audits;
- day-to-day knowledge;
- management reviews, including, but not limited to, computer security reviews and summary management reviews;
- financial statement audits and findings;
- Department's 5-Year Systems Development Plan;
- problems identified through on-going initiatives;
- system change requests;
- problem(s) identified by user groups or councils;

- prior Summary Financial Management System reviews; and
- prior year FMS Evaluations

In some cases, a review of these types of documents could comprise the entirety of a test for a specific criterion. However, given the automated nature of the systems being tested, in many if not most cases, transaction testing will also be required. Regardless of the test techniques implemented, the design of each test should be documented in writing.

When designing tests for specific controls, sample sizes should be determined in the test plan. In general, when applying statistical sampling, the following factors should be taken into account: (1) desired confidence level, (2) importance/significance of the control being tested, and (3) ensuring that the selected sample size is representative of the population. These considerations will drive the determination of sample size for each control being tested.

## 2. Prepare and Track CAPs

If system testing reveals that the system does not adequately conform to a particular criterion, a CAP should be developed to address the non-conformance and formulate a plan to resolve it, thus bringing the system back into conformance. This CAP should be documented on the Action Tracking tab of the EAT. However, the Departmental element is still responsible for tracking the CAP and ensuring that the milestones it sets out for correction of the non-conformance are met.

If any of the non-conformances identified in the Entity Evaluation tab are determined to rise to the level of a [material non-conformance](#), a detailed CAP must be developed and tracked locally. A CAP Summary should be submitted with the annual [Assurance Memorandum](#). CAP Summaries should be prepared using the “HQ Assurance Memo Template” or “Field Assurance Memo Template” provided in conjunction with this guidance. Additional instructions for completing the CAP Summary are provided in [Section XI](#).

## 3. Document the Assessment

The Entity Evaluation tab of the EAT provides a uniform Department-wide mechanism for documenting the FMS Evaluation. For each of the OMB Circular A-127 Conformance Criteria listed on the Systems Evaluation tab, a basis of evaluation must be recorded. Please note that the OMB Circular A-127 Conformance Criteria are exactly the same as the twelve criteria listed above on which test design should be based.

For each of the twelve criteria, the [basis of evaluation](#) should briefly describe the type of test performed, its general design, and its outcome. If a physical examination of documents was performed, the names of the documents should be included in this description.

## 4. Report the Results

Results of the FMS Evaluation should be reported in the annual Assurance Memorandum. All material non-conformances that are revealed as a result of system testing must be reported in the Assurance Memorandum. A summary of remediation activities for each material non-conformance should be included in the CAP Summary and attached to the Assurance Memorandum.

Please see [Section XI](#) of this guidance for detailed instructions on how to compose and address the Assurance Memorandum.

## X. Mixed Systems Evaluation

OMB Circular A-127, *Financial Management Systems*, defines a “[mixed system](#)” as an information system that can support both financial and nonfinancial functions. Table 5 below provides the applicable mixed systems inventory.

Table 5: DOE Mixed Systems

| System   | System Owner(s) |
|--|-----------------|
| Funds Distribution System (FDS)                                      | CF-40           |
| Procurement Assistance and Data System (PADS)                        | MA              |
| Active Facilities Database   | CF-10           |
| Departmental Inventory Management System (DIMS)                      | NNSA-NA-73      |
| Integrated Planning, Accountability and Budgeting System (IPABS)     | EM-62           |
| Facilities Information Management System (FIMS)                      | MA-50           |
| iManage Strategic Integrated Procurement Enterprise System (STRIPES) | CF-40           |
| Funds Controls and Distribution System (FCDS)                        | NNSA NA-MB-1    |
| Budget Execution and Reporting System (BEARS)                        | OR              |
| Vendor Inquiry Payment Electronic Reporting System (VIPERS)          | OR              |
| Vendor Invoice Approval System (VIAS)                                | OR              |
| iBenefits  | CF-40           |

### A. Mixed System Evaluation Process

The evaluation of [mixed systems](#) generally follows the same four-step process used for the [Entity Evaluation](#), described in [Section VIII](#) of this guidance. These four steps are:

1. Perform the Assessment;
2. Prepare and Track [CAPs](#);
3. Document the Assessment; and
4. Report the Results.

#### 1. Perform the Assessment

Departmental elements that are designated as owners of the [mixed systems](#) listed in Table 5 above must design and perform tests of those systems. These tests should be designed to evaluate the degree to which each system meets the criteria below.

1. System adheres to design, development, operation, and maintenance requirements.
2. System incorporates Government Information Security Reform Act and other government-wide computer security requirements.
3. System is supported by up-to-date system documentation adequate for user needs.
4. System contains appropriate internal controls.
5. Adequate system training and user support services are provided.
6. Ongoing maintenance of system is conducted for continued effective and efficient operations.

There are three common test techniques that can be implemented to perform the necessary tests required for an evaluation of a mixed system:

1. Direct observation of performance of the control.
2. Physical examination or inspection of documents.
3. Transaction testing and re-performance, the latter being most commonly used when testing automated controls.

In implementing the physical examination of documents test technique, managers should consider a variety of existing information at their disposal. Examples of such sources of information are:

- results of external audits;
- day-to-day knowledge;
- management reviews, including, but not limited to, computer security reviews and summary management reviews;
- Department's 5-Year Systems Development Plan;
- problems identified through on-going initiatives;
- system change requests;
- problem(s) identified by user groups or councils; and
- prior system reviews.

In some cases, a review of these types of documents could comprise the entirety of a test for a specific criterion. However, given the automated nature of the systems being tested, in many if not most cases, transaction testing will also be required. Regardless of the test techniques implemented, the design of each test should be documented in writing.

When designing tests for specific controls, sample sizes should be determined in the test plan. In general, when applying statistical sampling, the following factors should be taken into account: (1) desired confidence level, (2) importance/significance of the control being tested, and (3) ensuring that the selected sample size is representative of the population. These considerations will drive the determination of sample size for each control being tested.

## **2. Prepare and Track CAPs**

If system testing reveals that the system does not adequately conform to a particular criterion, a CAP should be developed to address the reportable condition and formulate a plan to resolve it, thus bringing the system back into conformance. This CAP should be documented on the Action Tracking tab of the EAT. However, the Departmental element is still responsible for tracking the CAP and ensuring that the milestones it sets out for correction of the reportable condition are met.

If any of the reportable conditions identified in the Entity Evaluation tab are determined to rise to the level of a significant deficiency, detailed CAP must be developed and tracked locally. A CAP Summary should be submitted with the annual [Assurance Memorandum](#). CAP Summaries should be prepared using the "HQ Assurance Memo Template" or "Field Assurance Memo Template" provided in conjunction with this guidance. Additional instructions for completing the CAP Summary are provided in [Section XI](#).

### 3. Document the Assessment

The Entity Evaluation tab of the EAT provides a uniform Department-wide mechanism for documenting the system Evaluation. For each of the OMB Circular A-127 Conformance Criteria listed on the Systems Evaluation tab, a basis of evaluation must be recorded for only those six criteria applicable to a [mixed system](#).

For each of the six criteria, the [basis of evaluation](#) should briefly describe the type of test performed, its general design, and its outcome. If a physical examination of documents was performed, the names of the documents should be included in this description.

### 4. Report the Results

Results of the system evaluation should be reported in the annual Assurance Memorandum. All significant deficiencies that are revealed as a result of system testing must be reported in the Assurance Memorandum. A summary of remediation activities for each significant deficiency should be included in the CAP Summary and attached to the Assurance Memorandum.

Please see [Section XI](#) of this guidance for detailed instructions on how to compose and address the Assurance Memorandum.

## XI. Annual Assurance Memorandum

Each [Departmental element](#) is required to report and submit an annual [Assurance Memorandum](#), which captures the results of annual [FMA Evaluation](#), [Entity Evaluation](#), and [FMS Evaluation](#). The Assurance Memorandum provides reasonable assurance that [internal controls](#) are working effectively and efficiently, and that operations are maintained in a manner consistent with applicable laws and regulations. The Assurance Memorandum will further identify any significant [control deficiencies](#) which might qualify that assurance, as defined in [Section C](#), and will be accompanied by a summary of the [corrective action plans](#) developed to address such issues.

To facilitate early communication of any significant control deficiencies identified during the internal controls evaluation process, the OCFO will be hosting a mid-year status update with each reporting entity. Staff from the Office of Financial Risk, Policy & Controls will participate in individual conference calls with FMFIA points of contact for each reporting entity in mid-April. These calls will be an opportunity for each reporting entity to share any control deficiencies identified to date in the evaluation process that may be reported as reportable conditions or material weaknesses in the entity's Assurance Memorandum, if not fully remediated by the end of the fiscal year.

### A. Reporting Documentation and Transmittal Methods

Each Departmental element will provide an Assurance Memorandum and selected other documents/files depending on the extent of evaluations required. In addition, certain documents will have different and/or multiple transmittal methods. Table 6 below provides specific instructions for transmitting required documentation.

Table 6: Reporting Documentation Transmittal Methods

| Document   | Format            | Method              | Recipient(s)  |
|--|-------------------|---------------------|---|
| <b>Assurance Memorandum (Including Corrective Action Plan Summary)</b> | Signed PDF        | Electronic Delivery | Field Office Assurance Memorandum addressed To: Lead Program Secretarial Office with copies to the Cognizant Secretarial Office(s).                     |
|  | Signed PDF        | Upload to iPortal   | Headquarters Assurance Memorandum addressed To: The Secretary, Thru: Appropriate Under Secretary and uploaded to the Internal Controls Space on iPortal |
| <b>Entity Assessment Tool (EAT)</b>                                    | Excel File / Tool | Upload to iPortal   | Internal Controls Space on iPortal  |
| <b>FMA Tool</b>  | Excel File / Tool | Upload to iPortal   | Internal Controls Space on iPortal – Please note that the federal staff field locations will be responsible for uploading files for its contractors.    |
| <b>FMA QA Results</b>  | Excel File / Tool | Upload to iPortal   |   |

## B. Format for the Assurance Memorandum

A separate electronic macro-enabled attachment to this guidance provides the required templates for preparing the Assurance Memorandum. There are two templates, one for field offices and one for headquarters offices. Please ensure that the appropriate template is used.

The Assurance Memorandum consists of two main sections:

1. The Main Body – Contains the actual assurance statements and executive summaries of any reportable control deficiencies.
2. The CAP Summary – Provides a listing of action plans for each reportable condition, material weakness, and/or material non-conformance reported in the Assurance Memorandum. The CAP Summary should briefly describe the remediation activities that have already taken place and/or those that will be implemented in the next fiscal year. The CAP Summary is segregated into: (a) New Issues/Action Plans; and (b) Action Plans from prior year reporting (may be open or closed). For action plans remediating deficiencies reported in previous years that have been closed in FY 2013, the CAP Summary should also include a statement noting the closure of the CAP.

Final responsibility for making assurances that financial, entity, and financial management systems internal controls are effective and efficient, produce reliable financial reports, and are compliant with all applicable laws and regulations, lies with the head of each Departmental element. As such, the **Assurance Memorandum must be signed by the head of the Departmental element.**

## C. Determining Issues to be Reported

In the Assurance Memorandum, control deficiencies that meet certain criteria must be reported. In a typical control assessment, control deficiencies may be identified; however, only certain issues need to be specifically discussed and referenced in the Assurance Memorandum. Table 7 below provides a description of the types of issues to be reported for each section of the Assurance Memorandum, a

definition for each issue type, and an indication of which issue types should be reported in the Assurance Memorandum (with corrective action plans).

*Table 7: Definitions of Control Issues*

| <b>Control Issue Type</b>                                | <b>Definition</b>  | <b>Reported in Assurance Memorandum?</b> |
|--|--|--|
| <i>Financial Management Assurance Evaluation</i>         |  |  |
| Reportable Condition                                     | A control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report external financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements, or other significant financial reports, that is more than inconsequential, will not be prevented or detected. | Yes                                      |
| Material Weakness  | Reportable condition, or combination of reportable conditions, that results in more than a remote likelihood that a material misstatement of the financial statements, or other significant financial reports, will not be prevented or detected.  | Yes                                      |
| <i>American Recovery and Reinvestment Act Evaluation</i> |  |  |
| Reportable Condition                                     | A control deficiency which would impact the reporting entity's ability to make the following assurances:<br><br>ARRA funding has been expended for the intended purposes and in accordance with internal and external guidance; Reported results regarding the expenditure of funds and the outcomes achieved are accurate and verifiable; OR Key processes impacting the execution of ARRA funding have been evaluated and are deemed effective.                                  | Yes                                      |
| <i>Entity Evaluation and Mixed Systems</i>               |  |  |
| Reportable Condition                                     | A control deficiency, or combination of control deficiencies, that in management's judgment should be communicated because they represent significant weaknesses in the design or operation of internal controls that could adversely affect the organization's ability to meet its internal control objectives.   | Yes                                      |
| Material Weakness  | Reportable conditions which the head of the Departmental Element determines to be significant enough to report outside of their department.  | Yes                                      |

| Control Issue Type                             | Definition   | Reported in Assurance Memorandum? |
|--|--|-----------------------------------|
| <i>Financial Management Systems Evaluation</i> |  |                                   |
| Material Non-Conformance                       | Exists when financial systems do not substantially comply with federal financial management system requirements OR where local control deficiencies impact financial systems ability to comply. The EAT Tool defines the criteria against which conformance is evaluated and captures identified non-conformances.     | Yes                               |
| <i>All Evaluations</i>                         |  |                                   |
| Control Deficiency                             | Exists when specific control objectives are not being met. This could be due to a deficiency in the design or operations of controls and may result in risk occurrence. Control deficiencies are only reportable if they meet the definition of a Reportable Condition or Material Weakness.                           | No                                |
| Scope Limitation                               | Exists when the Entity has identified potentially significant deficiencies in the scope of the internal controls evaluations conducted, which would warrant disclosure to ensure limitations are understood. Scope limitations may be determined by the entity or may be required by the CFO in certain circumstances. | Yes                               |

Table 8: Listing of Required Internal Control Evaluations by Departmental Element

| Departmental Element  |   | FMA<br>Evaluation | ARRA | Entity<br>Evaluation | FMS | Mixed<br>System |
|---|---|-------------------|------|----------------------|-----|-----------------|
| F<br>I<br>E<br>L<br>D<br>O<br>F<br>F<br>I<br>C<br>E<br>S                                    | Bonneville Power Administration             | ✓                 |      | ✓                    | ✓   |                 |
|   | Chicago Office                              | ✓                 | ✓    | ✓                    |     |                 |
|   | Consolidated Business Center                | ✓                 | ✓    | ✓                    |     |                 |
|   | Golden Field Office                         | ✓                 | ✓    | ✓                    |     |                 |
|   | Idaho Operations Office                     | ✓                 | ✓    | ✓                    |     |                 |
|   | National Energy Technology Laboratory       | ✓                 | ✓    | ✓                    |     |                 |
|   | Naval Petroleum Reserves – Casper           |                   |      | ✓                    |     |                 |
|   | Naval Reactors Laboratory Field Office      | ✓                 |      | ✓                    |     |                 |
|   | Oak Ridge Office                            | ✓                 | ✓    | ✓                    |     | ✓               |
|   | Office of River Protection                  |                   |      | ✓                    |     |                 |
|   | Richland Operations Office                  | ✓                 | ✓    | ✓                    |     |                 |
|   | Savannah River Operations Office            | ✓                 | ✓    | ✓                    |     |                 |
|   | Southeastern Power Administration           | ✓                 |      | ✓                    | ✓   |                 |
|   | Southwestern Power Administration           | ✓                 |      | ✓                    | ✓   |                 |
|   | Strategic Petroleum Reserve Office          | ✓                 |      | ✓                    |     |                 |
|   | Western Area Power Administration           | ✓                 | ✓    | ✓                    | ✓   |                 |
| H<br>E<br>A<br>D<br>Q<br>U<br>A<br>R<br>T<br>E<br>R<br>S<br>O<br>F<br>F<br>I<br>C<br>E<br>S | Advanced Research Project Agency–Energy     | ✓                 | ✓    | ✓                    |     |                 |
|   | Chief Financial Officer                     | ✓                 | ✓    | ✓                    | ✓   | ✓               |
|   | Chief Information Officer                   | ✓                 |      | ✓                    |     |                 |
|   | Congressional and Intergovernmental Affairs |                   |      | ✓                    |     |                 |
|   | Economic Impact and Diversity               |                   | ✓    | ✓                    |     |                 |
|   | Electricity Delivery and Energy Reliability | ✓                 | ✓    | ✓                    |     |                 |
|   | Energy Efficiency and Renewable Energy      | ✓                 | ✓    | ✓                    |     |                 |
|   | Energy Information Administration           |                   |      | ✓                    |     |                 |
|   | Environmental Management                    | ✓                 | ✓    | ✓                    |     | ✓               |
|   | Federal Energy Regulatory Commission        |                   |      | ✓                    | ✓   |                 |
|   | Fossil Energy                               | ✓                 | ✓    | ✓                    |     |                 |
|   | General Counsel                             |                   |      | ✓                    |     |                 |
|   | Health, Safety and Security                 |                   |      | ✓                    |     |                 |
|   | Hearings and Appeals                        |                   |      | ✓                    |     |                 |
|   | Human Capital Management                    | ✓                 |      | ✓                    |     |                 |
|   | Indian Energy Policy & Programs             |                   |      | ✓                    |     |                 |
|   | Inspector General                           |                   |      | ✓                    |     |                 |
|   | Intelligence and Counterintelligence        |                   |      | ✓                    |     |                 |
|   | Legacy Management                           | ✓                 |      | ✓                    |     |                 |
|   | Loan Program Office                         | ✓                 | ✓    | ✓                    |     |                 |
|   | Management                                  | ✓                 | ✓    | ✓                    |     | ✓               |
|   | National Nuclear Security Administration    | ✓                 | ✓    | ✓                    |     | ✓               |
|   | Nuclear Energy                              | ✓                 |      | ✓                    |     |                 |
|   | Policy and International Affairs            |                   |      | ✓                    |     |                 |
|   | Public Affairs                              |                   |      | ✓                    |     |                 |
|   | Science                                     | ✓                 | ✓    | ✓                    |     |                 |

## XII. Glossary

**Assurance Memorandum** Annual statement of assurance over the status of internal controls made by each Departmental element.

For further details regarding the required content of the Assurance Memorandum, please see [Section XI](#).

**Basis of Evaluation** Represents the key information and/or activities leveraged/performed to provide reliable support for assurances that the control objectives and considerations have been addressed.

The Basis of Evaluation must be a tangible and documented activity to be valid. Examples include: transaction testing, safety managers' reports, annual infrastructure reports, bi-annual workforce planning survey results, other reports, memos, reviews, assessments, evaluations, or plans, emails, meeting minutes, agendas, certificates, newsletters, bulletin boards, documented signatures, etc.

**Combined Risk Assessment** The residual risk considering the control environment. A measure of the end risk to DOE. For FMA evaluations, this is a quantitative measure of residual risk. For Entity evaluations, please refer to the definition for "[residual risk](#)."

In the FMA Tool, the combined risk is a calculated field based on exposure risk and control risk, as well as the presence of risk factors. If no control testing has been performed, the combined risk will default to the risk exposure risk rating. If a risk factor is indicated to be present in the current year (e.g. system change, process change), then the combined risk will default to "unknown" (UNK), until controls are tested and the control risk is identified. Once control risk is identified, the Combined Risk will automatically calculate.

**H** – High risk, poor risk mitigation.

**M** – Moderate risk.

**L** – Low risk, effective risk mitigation.

Risks with a low exposure rating are not required to have a control rating determination. Thus, a combined risk rating is not necessary and testing for those risks is not required within the prescribed test cycle.

The diagram below demonstrates the calculation of **High**, **Moderate**, and **Low** combined risk ratings.

|               |   |          |          |          |
|---------------|---|----------|----------|----------|
| Exposure Risk | H | Moderate | High     | High     |
|               | M | Low      | Moderate | Moderate |

|  |   |                     |           |           |
|--|---|---------------------|-----------|-----------|
|  | L | No rating           | No rating | No rating |
|  |   | L                   | M         | H         |
|  |   | <b>Control Risk</b> |           |           |

### Control Deficiency

Control deficiencies exist when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. A design deficiency exists when a control necessary to meet the control objective is missing or an existing control is not properly designed, so that even if the control operates as designed the control objective is not always met. An operation deficiency exists when a properly designed control does not operate as designed or when the person performing the control is not qualified or properly skilled to perform the control effectively.

### Control Execution

A rating resulting from individual control testing.

As defined in the FMA Tool:

- 1 – Passed with no failures.
- 2 – Passed with failures within acceptable threshold.
- 3 – Failed.

Entity control tests may apply these ratings, or other ratings developed by each organization.

### Control Objective

Identifies the key objectives to be achieved by the internal control in each area, as well as specific types of control issues that should be considered when performing the evaluation.

Specific end to be achieved to ameliorate, minimize, manage, or mitigate risks. Each objective takes into consideration the nature of the activity, the organization's mission, and the cost/benefits of each control technique in determining desired control objectives.

The positive things agency managers want to have happen or the negative things managers want to prevent from happening.

### Control Risk Assessment

A measure of the risk considering the effectiveness of the controls to mitigate that risk and the risk occurrence.

In the FMA Tool, control risk is a calculated field based on Risk Occurrence and Control Set Execution. The diagram below demonstrates the calculation of **High**, **Moderate**, and **Low** control risk ratings.

Apply the ratings in the following table:

|                 |   |                       |          |          |
|-----------------|---|-----------------------|----------|----------|
| Risk Occurrence | 3 | High                  | High     | High     |
|                 | 2 | Moderate              | Moderate | High     |
|                 | 1 | Low                   | Moderate | Moderate |
|                 |   | 1                     | 2        | 3        |
|                 |   | Control Set Execution |          |          |

**Control Set Execution:** Rating based on assessment testing results of all individual controls within a control set.

**1** - Passed with no failures;

**2** - Passed with failures within acceptable threshold; or

**3** - Failed.

**Risk Occurrence:** Determined during dual-purpose testing.

**1** - No risk occurrence;

**2** - Risk occurred within acceptable threshold; or

**3** - Risk occurred outside the acceptable threshold.

#### Corporate Risk

A risk that is pre-populated into the FMA Tool to facilitate the FMA Evaluation. The FMA tool also allows each Departmental element to add any additional locally-identified risks to the tool.

#### Corrective Action Plan

A plan of action to correct an internal control deficiency. A CAP must be prepared and tracked for all control deficiencies identified during the internal controls evaluation process. A CAP Summary for reportable conditions identified in the Memorandum of Assurance must be submitted along with the memorandum.

#### Departmental Element

Refers to Department of Energy headquarters mission and mission support offices and field and operation offices, and all DOE Agencies. This includes all contractors.

#### Dual-purpose Testing

A testing mechanism designed to evaluate both control execution (i.e. did the control operate as intended) and risk occurrence (i.e. is there evidence that the stated risk occurred). Dual-purpose testing provides a mechanism for ensuring controls are actually effective in risk mitigation, thereby reinforcing the control design effectiveness decision.

#### Entity

Related to the organizational level. Pertaining primarily to functions or controls that are non-financial in nature, (e.g. administrative, operational, or programmatic).

**Entity Assessment Tool (EAT)**

The primary system for documenting and reporting on the results of evaluations and testing of entity and financial management systems risks and controls.

**Entity Evaluation**

Detailed evaluation of an organization's key administrative, operational, or programmatic activities, to determine whether adequate control techniques exist and are implemented to achieve cost-effective compliance with FMFIA.

**Exposure Risk Assessment**

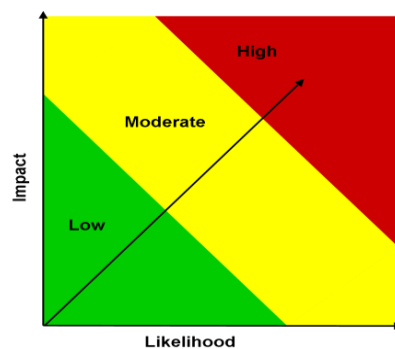
A combined measure of the likelihood and impact to DOE should the risk occur (regardless of the strength of the controls to mitigate the risk, given the general environment).

In the FMA Tool, this is a professional judgment rating of **H**(igh), **M**(oderate), **L**(ow), or **NR** (not relevant). The NR rating is for corporately defined risks that may not impact your location. No assessment is required with a rating of NR.

**General environment:** Environment that assumes no mitigating controls are in place.

**Likelihood:** The measure of the relative potential that the risk might occur given the general environment.

**Impact:** The measure of the magnitude and nature of the effect the risk might cause given the general environment.



**Federal Managers' Financial Integrity Act (FMFIA)**

DOE Order 413.1b, *Internal Control Program* requires the Department to establish and maintain an internal control program to evaluate internal controls and report the status of major problems up through the chain of command to the President and Congress. To support Departmental reporting, Heads of Departmental elements, including the National Nuclear Security Administration (NNSA), are required to report on the status of their organization's internal controls, including reportable problems identified and progress made in correcting prior reportable problems.

FMFIA provides for:

- Evaluation of an agency's internal controls in accordance with GAO standards.
- Annual reporting by the head of each executive agency to the President.
- Identification of material weaknesses and the plans for correcting them.
- Agencies to provide for internal control assessments on an on-going basis.

**Financial Management Assurance (FMA) Evaluation**

An evaluation of internal controls over financial reporting that tests these controls to ensure effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.

**Financial Management Assurance (FMA) Tool**

The primary system for documenting and reporting on the results of evaluations and testing of financial management reporting risks and controls.

**FMA Quality Assurance (QA) Tool and Report**

A macro-enabled Excel tool that is run from within a standard reporting package distributed by CF-50 to Departmental FMA contacts. After running the QA Tool, a report is created that houses the results of the review. The QA Tool highlights potential data anomalies for management review, and also includes an area for comments in the Table of Contents, for management to discuss the results.

**Financial Management Systems**

OMB Circular A-127, *Financial Management Systems*, defines a financial system as a "core financial system" that may perform all financial functions and is the system of record that maintains all transactions resulting from financial events.

**Financial Management Systems (FMS) Evaluation**

In accordance with the FMFIA, Departmental elements with financial management systems included in the Department's FMS Inventory are required to conduct an FMS Evaluation as part of their annual internal controls review process.

**Focus Area**

***In the FMA Evaluation***

Areas of emphasis which require additional assessment within the year. Risks identified in focus areas within the FMA Tool will default to "Y" in the "Corporate Request" (Corp. Req) column of the Assessment Tab worksheet.

***In the Entity Evaluation***

The 10 cross-cutting control areas picked from the 22 GAO control areas that represent high risk control activities for ensuring an agency meets its core mission objectives. When issues are identified in these control areas, a more detailed impact assessment will be required to support corporate consolidation and reporting.

**High Combined Risk**

A risk in the FMA Tool that is determined to have:

1. Moderate control risk rating and high exposure risk rating. OR

2. High control risk rating and high exposure risk rating.

|                                    |   |
|------------------------------------|---|
| <b>Impact Assessment</b>           | An evaluation of the impact of a breakdown in a particular control identified in the EAT. This evaluation includes a description of the general breakdown in the control, the program(s) and sub-program(s) affected by the breakdown, and the nature and significance of the impact. The impact assessment is documented using the Impact Assessment Tab in the EAT.   |
| <b>Internal Control</b>            | <p>An integrated component of an organization's management that provides reasonable assurance that the following objectives are being achieved.</p> <ul style="list-style-type: none"><li>• Effectiveness and efficiency of operations.</li><li>• Reliability of financial and program reporting.</li><li>• Compliance with applicable laws and regulations.</li></ul>  |
| <b>Key Control</b>                 | A control, or set of controls, that address the relevant assertions for a material activity (e.g., financial statement line item) or significant risk. At the point that management is ready to test controls, and in order to focus test work, management must identify the key controls in place.   |
| <b>Material Non-conformance</b>    | Exists when <i>financial systems</i> do not substantially comply with federal financial management system requirements OR where local control deficiencies impact financial systems' ability to comply. The EAT defines the criteria against which conformance is evaluated and captures identified non-conformances.   |
| <b>Material Weakness</b>           | <p><b>Non-Financial-</b> Reportable conditions which the head of the Departmental element determines to be significant enough to report.</p> <p><b>Financial reporting</b> - Reportable condition, or combination of reportable conditions, that results in more than a remote likelihood that a material misstatement of the financial statements, or other significant financial reports, will not be prevented or detected.</p>  |
| <b>Minimum Evaluation Standard</b> | The basis by which testing cycles for the FMA Evaluation are determined. The minimum evaluation standard for FY 2013 is based on the combined risk rating of risks identified (both corporate risks automatically populated by the FMA Tool and local risks identified by the individual Departmental element) for each standard process and sub-process. Controls for processes that have risks with a combined risk rating of High must be tested each year. Controls for a process that have risks with a combined risk rating of moderate must be tested at least once every two years. Controls for processes that have risks with a combined risk rating of low must be tested at least once every three years. |
| <b>Mitigate</b>                    | To put controls in place that would ensure the probability and/or impact of a given risk is as low as possible.   |

|   |  |
|---|--|
| <b>Mixed System</b>                             | OMB Circular A-127, <i>Financial Management Systems</i> , defines a mixed system as an information system that can support both financial and nonfinancial functions   |
| <b>OMB Circular A-123, including Appendix A</b> | OMB Circular A-123 prescribes the guidelines for evaluating, improving, and reporting on internal controls. Appendix A requires an annual assurance statement on Internal Controls Over Financial Reporting (ICOFR).   |
| <b>Reasonable Assurance</b>                     | Judgment by management based upon available information that the systems of internal controls are operating as intended under FMFIA.   |
| <b>Remediation Activity</b>                     | An action put in place that would address the correction of a controls deficiency identified through an internal controls assessment.  |
| <b>Reportable Condition</b>                     | <p><b>Non-Financial</b> – A control deficiency, or combination of control deficiencies, that in management’s judgment should be communicated because they represent significant weaknesses in the design or operation of internal control that could adversely affect the organization’s ability to meet its internal control objectives.</p> <p><b>Financial reporting</b> - A control deficiency, or combination of control deficiencies, that adversely affects the entity’s ability to initiate, authorize, record, process, or report external financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity’s financial statements, or other significant financial reports, that is more than inconsequential will not be prevented or detected.</p> <p><b>ARRA:</b> A control deficiency which would impact the reporting entity’s ability to make the following assurances:</p> <ul style="list-style-type: none"> <li>• ARRA funding has been expended for the intended purposes and in accordance with internal and external guidance;</li> <li>• Reported results regarding the expenditure of funds and the outcomes achieved are accurate and verifiable; or</li> <li>• Key processes impacting the execution of ARRA funding have been evaluated and are deemed effective.</li> </ul> |
| <b>Residual Risk</b>                            | The risk that remains after a risk response is executed.   |
| <b>Risk Assessment</b>                          | A review of the susceptibility of a program or function to the occurrence of waste, loss, or unauthorized use, or misappropriation. The potential for risks to an organization may be internal or external, or both. The possibility of suffering harm or loss.  |
| <b>Risk Factor</b>                              | Refers to the identification of changes that may affect the exposure risk and/or effectiveness of the existing controls in mitigating the risk. Risk factors include system changes, process changes, organization changes,  |

other changes (i.e., audit, IG, GAO, etc.).

In the FMA Tool, the identification of risk factors changes the combined risk assessment in the FMA Tool to “UNK” (unknown) and requires analysis and/or retesting.

**Risk Response**

A determination by management on how a risk should be managed. Management must take into consideration the potential impact of the risk and the likelihood of occurrence, as well as the cost associated with mitigating the risk.

Types of risk responses:

**Accept** – No action is taken to affect risk likelihood or impact.

**Avoid** – Exiting the activities that give rise to risk. This may involve changing project scope, using an alternate technology, selecting a different vendor or product, or canceling an initiative.

**Reduce** – Action is taken to reduce risk likelihood or impact, or both, to mitigate a risk to an acceptable level. Typically performed through the placement of controls or other risk management activities.

**Share** – Reducing the likelihood or impact of a risk by sharing a portion of the risk with another organization. This may include forming partnerships with other organizations that have a “stake” in the success of a mission objective.

**Transfer** – Changing ownership of a risk from one organization to another; typically done through written acknowledgment.

**Risk Tolerance**

The level of variation in performance that management is willing to accept, relative to achieving its objectives. Management should establish its risk tolerance level before the placement of controls.

**Scope Limitation**

Exists when the Entity has identified potentially significant deficiencies in the scope of the internal controls evaluations conducted, which would warrant disclosure to ensure limitations are understood. Scope limitations may be determined by the entity or may be required by the CFO in certain circumstances.

**Standard Process**

A process that is pre-populated in the FMA Tool and is required to be tested during the FMA Evaluation.

**Standard Sub-process**

A component of a standard process, also pre-populated in the FMA Tool.

**Statement of Assurance**

An annual statement required by the Federal Managers’ Financial Integrity Act (FMFIA) that represents the Secretary’s informed judgment as to the overall adequacy and effectiveness of internal controls within the Department. The statement reports the results of evaluations made on the

Department's entity, financial, and financial management systems controls, including any material weaknesses and/or material non-conformances identified during the fiscal year. Also, updates of corrective action progress made on existing material weaknesses and material non-conformances are included in the statement. The annual Statement of Assurance is included in the Department's Agency Financial Report. This statement is generally based on the fiscal year period from October through September.

**Testing Activity**

A procedure to determine whether internal control systems are working in accordance with internal control objectives.